INTERNAL REVENUE SERVICE
IRS News Release

Media Relations Office | Washington, D.C. | Media Contact: 202.622.4000
www.IRS.gov/newsroom | Public Contact: 800.829.1040

Electronic Federal Tax Payment System Cited in New E-mail Scam

IR-2006-116, July 19, 2006

WASHINGTON — The Internal Revenue Service is warning taxpayers to be on the lookout for a new e-mail scam that uses the Treasury Department's Electronic Federal Tax Payment System (EFTPS) as a hook to lure individuals into disclosing their personal information.

The system, which is used by more than six million taxpayers, allows businesses and individuals to pay all their federal taxes online or by phone.

The new e-mail scam, fraught with grammatical errors and typos, looks like a page from IRS.gov and claims to be from the "IRS Antifraud Comission" (sic), a fictitious group. The e-mail claims someone has enrolled the taxpayer's credit card in EFTPS and has tried to pay taxes with it. The e-mail also says there have been fraud attempts involving the taxpayer's bank account. The e-mail claims money was lost and "remaining founds" (sic) are blocked. Recipients are asked to click on a link that will help them recover their funds, but the subsequent site asks for personal information that the thieves could use to steal the taxpayer's identity.

"The IRS does not send out unsolicited e-mails asking for personal information," said IRS Commissioner Mark W. Everson. "Don't be taken in by these criminals."

Additionally, the IRS never asks people for the PIN numbers, passwords or similar secret access information for their credit card, bank or other financial accounts.

This latest e-mail scam is the first one known to reference EFTPS.

The IRS has seen a recent increase in these scams. Since November, 104 different scams have been identified, with 22 of those coming in June, the most since 40 were identified in March during the height of the filing season.

Many of these schemes originate outside the United States. To date, investigations by the Treasury Inspector General for Tax Administration have identified sites hosting more than two dozen IRS-related phishing scams. These scam Web sites have been located in many different countries, including Argentina, Aruba, Australia, Austria, Canada, Chile, China, England, Germany, Indonesia, Italy, Japan, Korea, Malaysia, Mexico, Poland, Singapore and Slovakia, as well as the United States.

Other scams claim to come from the IRS, tell recipients that they are due a federal tax refund, and direct them to a Web site that appears to be a genuine IRS site. The bogus sites contain forms or interactive Web pages similar to IRS forms or Web pages but which have been modified to request detailed personal and financial information from the e-mail recipients.

Tricking consumers into disclosing their personal and financial information, such as secret access data or credit card or bank account numbers, is fraudulent activity which can result in identity theft. Such schemes perpetrated through the Internet are called “phishing” for information.

The information fraudulently obtained is then used to steal the taxpayer’s identity and financial assets. Typically, identity thieves use someone’s personal data to empty the victim’s financial accounts, run up charges on the victim’s existing credit cards, apply for new loans, credit cards, services or benefits in the victim’s name and even file fraudulent tax returns.

When the IRS learns of new schemes involving use of the IRS name or logo, it issues consumer alerts warning taxpayers about the schemes.

The IRS also has established an electronic mailbox for taxpayers to send information about suspicious e-mails they receive which claim to come from the IRS. Taxpayers should send the information to: phishing@irs.gov.

More than 8,000 bogus emails have been forwarded to the IRS, with nearly 1,300 forwarded in June alone.

The IRS’s mail box allows taxpayers to send copies of possibly fraudulent e-mails involving misuse of the IRS name and logo to the IRS for investigation. Instructions on how to properly submit one of these communications to the IRS may be found on the IRS Web site at www.irs.gov. Enter the term "phishing" in the search box in the upper right hand corner. Then open the article titled “How to Protect Yourself from Suspicious E-Mails” and scroll through it until you find the instructions. Following these instructions helps ensure that the bogus e-mails relayed by taxpayers retain critical elements found in the original e-mail. The IRS can use the information, URLs and links in the bogus e-mails to trace the hosting Web sites and alert authorities to help shut down these fraudulent sites.

However, due to the volume the mailbox receives, the IRS cannot acknowledge receipt or reply to taxpayers who submit their bogus e-mails. The phishing@irs.gov mailbox is only for suspicious e-mails and not for general taxpayer contact or inquiries.

For information on preventing or handling the aftermath of identity theft, visit the Federal Trade Commission’s consumer (http://www.consumer.gov/idtheft/index.html) and OnGuardOnLine (http://onguardonline.gov/index.html) Web sites. Click on "Topics" to find the identity theft and phishing areas on OnGuardOnLine.

For information on identity theft prevention and victim assistance in relation to tax administration, visit the IRS Identity Theft Web page which can be found on IRS.gov. Enter the term "identity theft" in the search box in the upper right hand corner.

For schemes other than phishing, please report the fraudulent misuse of the IRS name, logo, forms or other IRS property by calling the Treasury Inspector General for Tax Administration’s toll-free hotline at 1-800-366-4484.

—30—